

AFFIDAVIT

I, Jay L. Stern, being duly sworn, depose and state:

1. I am a United States Postal Inspector with the United States Postal Inspection Service (USPIS) assigned to the Boston Division, in Providence, Rhode Island. I have been so employed since 1990. As a United States Postal Inspector, I am responsible for the investigation of Federal offenses involving the transportation, distribution, receipt, and sale of child pornography through United States mail in violation of 18 U.S.C. §§ 2252 and 2252A. I have participated in the investigation of child pornography cases over the course of my career, and since April 1, 2007, I have specifically been assigned to investigate these crimes. I am currently assigned to the Rhode Island Internet Crimes Against Children (ICAC) task force. I have received training in the investigation of child exploitation cases by attending training courses and seminars. Further, I am authorized and assigned to investigate violations of federal criminal law, including 18 U.S.C. § 2252 et seq.

2. I am investigating the activities of Donald J. Jones, DOB: 1964. As will be shown below, there is probable cause to believe that Donald J. Jones intends to travel to the District of Rhode Island from the District of New Jersey on April 8, 2011, for purposes of engaging in illicit sexual conduct as defined in 18 U.S.C. § 2423(f), in violation of 18 U.S.C. §§2423(b) and (f); that while in the District of New Jersey, and more specifically, the two premises listed in this search warrant, he has used a facility and means of interstate commerce, to wit, the Internet, to persuade, induce, entice, and coerce an individual, who was at that time purporting to be under the age of 18 years, to engage in sexual activity for which any person can be charged with a criminal offense, to wit, sexual penetration by a person eighteen (18) years of

age or older with another person fourteen (14) years of age or younger, in violation of Rhode Island General Laws §§11-37-8.1; in violation of 18 U.S.C. § 2422(b); and that from the listed premises in the District of New Jersey, he has knowingly distributed visual depictions that had been mailed, shipped and transported in interstate or foreign commerce, by computer, the producing of such visual depictions having involved the use of minors engaging in sexually explicit conduct, as defined in 18 U.S.C. §2256(2)(A), and such depictions being of such conduct, in violation of 18 U.S.C. §§ 2252(a)(2) and (b)(1). Your affiant is further aware that Donald Jones has three State of New Jersey convictions for crimes against children which include child endangerment and aggravated sexual assault of a child under the age of thirteen.

Subject To Be Arrested and Locations To Be Searched

3. I am submitting this affidavit in support of a search warrant authorizing a search of the subject locations as further described below:

- a) Any and all personal possessions and luggage, including, but not limited to, a laptop computer in the possession of Donald Jones, arriving in Rhode Island on April 8, 2011;
- b) Cellular telephone serviced by AT&T Wireless, assigned number (609) 845-5723;
- c) Cellular telephone serviced by AT&T Wireless, assigned number (609) 288-0961;

for the items specified in Attachment B, which items constitute instrumentalities, fruits, and evidence of the foregoing violations. I am requesting authority to search the body of and possessions of Donald Jones, and the area within his control, including any computer and computer media located therein where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of crime.

This affidavit is also in support of an arrest warrant for Donald J. Jones.

4. The statements in this Affidavit are based in part on information provided by your affiant, Jay Stern, as well as other members of the USPIS, Immigration and Customs Enforcement Special Agent Jodie Donaghy, as well as other members of the Internet Crimes Against Children Task Force (ICAC).

5. Since this affidavit is being submitted for the limited purpose of securing search warrants, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§2423(b) and (f); 18 U.S.C. § 2422(b); 18 U.S.C. §§2252(a)(4) and (b)(2); and 18 U.S.C. §§ 2252(a)(2) and (b)(1), are presently located at the aforementioned premises and locations.

STATUTORY AUTHORITY

6. This investigation concerns alleged violations of 18 U.S.C. §§2423(b) and (f); 18 U.S.C. § 2422(b); 18 U.S.C. §§2252(a)(4) and (b)(2); and 18 U.S.C. §§ 2252(a)(2) and (b)(1), relating to the sexual exploitation of minors.

a. 18 U.S.C. § 2252(a)(1) prohibits knowingly transporting or shipping in interstate or foreign commerce, by computer or mail, any visual depiction of minors engaging in sexually explicit conduct.

b. 18 U.S.C. § 2252(a)(2) prohibits knowingly receiving or distributing, by computer or mail, any visual depiction of minors engaging in sexually explicit conduct that has been mailed, shipped, or transported in interstate or foreign commerce. That section also prohibits knowingly reproducing any visual depiction of minors engaging in sexually explicit conduct for distribution in interstate or foreign commerce by any means,

including by computer or the mail.

- c. 18 U.S.C. § 2252(a)(4) prohibits possessing one or more books, magazines, periodicals, films, or other materials which contain visual depictions of minors engaged in sexually explicit conduct that have been transported in interstate or foreign commerce, or that were produced using materials that had traveled in interstate or foreign commerce.
- d. 18 U.S.C. § 2252A(a)(1) prohibits knowingly mailing, transporting, or shipping child pornography in interstate or foreign commerce by any means, including by computer.
- e. 18 U.S.C. § 2252A(a)(2) prohibits knowingly receiving or distributing any child pornography that has been mailed or shipped or transported in interstate or foreign commerce by any means, including by computer.
- f. 18 U.S.C. § 2252A(a)(3)(A) prohibits a person from knowingly reproducing child pornography for distribution through the mail or in interstate or foreign commerce by any means, including by computer.
- g. 18 U.S.C. § 2252A(a)(3)(B) prohibits knowingly advertising, promoting, presenting, distributing, or soliciting through the mail, or using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means any material in a manner that reflects the belief or is intended to cause another to believe that the material is or contains a visual depiction of an actual minor engaging in sexually explicit conduct, or an obscene visual depiction of a minor engaging in sexually explicit conduct.
- h. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing any

book, magazine, periodical, film, videotape, computer disk, or other material that contains an image of child pornography that has been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer.

i. 18 U.S.C. §§2423(b) and (f) prohibits travel in interstate commerce for the purpose of engaging in illicit sexual conduct as defined in 18 U.S.C. § 2423(f), that is, a sexual act with a person under the age of 18 years of age that would be in violation of chapter 109A of the United States Code if the sexual act had occurred in the special maritime and territorial jurisdiction of the United States.

j. 18 U.S.C. § 2422(b) prohibits knowingly using or attempting to use a facility and means of interstate commerce, to wit, the Internet, to persuade, induce, entice, and coerce an individual, who was at that time purporting to be under the age of 18 years, to engage in sexual activity for which any person can be charged with a criminal offense.

DEFINITIONS

7. The following definitions apply to this Affidavit and Attachment C to this Affidavit:

- a. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.
- b. "Child Pornography" includes any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in

sexually explicit conduct; (b) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).

c. “Computer” refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.” *See* 18 U.S.C. § 1030(e)(1).

d. “Computer hardware” consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

e. “Computer passwords and data security devices” consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A

password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

f. “Computer-related documentation” consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

g. “Computer software” is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet.

i. “Minor” means any person under the age of 18 years. *See* 18 U.S.C. § 2256(1).

j. “Peer-to-peer file-sharing” (“P2P”) is a method of communication available to Internet users through the use of special software. Computers linked together through the

Internet using this software form a network that allows for the sharing of digital files between users on the network. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up files on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user's computer, and conducting searches for files that are currently being shared on another user's computer.

k. "Sexually explicit conduct" applies to visual depictions that involve the use of a minor, *see* 18 U.S.C. § 2256(8)(A), or that have been created, adapted, or modified to appear to depict an identifiable minor, *see* 18 U.S.C. § 2256(8)(C). In those contexts, the term refers to actual or simulated (a) sexual intercourse (including genital-genital, oral-genital, or oral-anal), whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person. *See* 18 U.S.C. § 2256(2)(A).

l. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

m. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); mechanical form (including, but not limited to, phonograph records, printing, typing); or electrical, electronic or magnetic form (including, but not limited to,

tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMC's"), memory sticks; optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

8. Computers and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images. To distribute these on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings and telephone calls.

9. The development of computers has changed this. Computers basically serve five functions in connection with child pornography: production, communication, distribution, storage, and social networking.

10. Child pornographers can now transfer photographs from a camera onto a computer-readable format with a device known as a scanner. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows

any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

11. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

12. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

13. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

14. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path

of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space -- that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space -- for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

15. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment.

This is almost always true because of the following two reasons:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment

of a laboratory is essential to its complete and accurate analysis.

16. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

SEARCH METHODOLOGY TO BE EMPLOYED

17. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- a. on-site triage of computer systems to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, as well as a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or potential victims;
- b. examination of all of the data contained in such computer hardware, computer software, or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;
- c. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement

personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

- d. surveying various file directories and the individual files they contain;
- e. opening files in order to determine their contents;
- f. scanning storage areas;
- g. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment C; and/or
- h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment C.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

18. Based upon my training and experience and on what I have been told by other Special Agents with experience and training in this field, the following traits and characteristics are generally found to exist and be true in cases involving individuals who collect child pornography:

- a. The majority of individuals who collect child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.
- b. The majority of individuals who collect child pornography collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual

gratification. The majority of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child pornography but which nonetheless fuel their deviant sexual fantasies involving children.

c. The majority of individuals who collect child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, P2P, e-mail, e-mail groups, bulletin boards, Internet Relay Chat (IRC), newsgroups, instant messaging, and other similar vehicles.

d. The majority of individuals who collect child pornography maintain books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide.

e. The majority of individuals who collect child pornography often collect, read, copy or maintain names, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on

computer storage devices, or merely on scraps of paper.

f. The majority of individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials. They almost always maintain their collections in the privacy and security of their homes or other secure location.

BACKGROUND OF THE INVESTIGATION

19. On March 21, 2011, while acting in an undercover capacity, your affiant observed the following posting on the site Motherless.com placed by an individual using the name "donjuan045":

Looking for white mothers and fathers who have young and would like to see their daughters get parted by a normal to moderate sized black pole

The title of this posting was "I am into young" and the individual who posted this wrote that he was a "Male 4 Female"; was from "Pennsylvania, US"; and was "Wanting a real life meeting". The picture associated with donjuan045's profile was that of a very young female, approximately 4 to 6 years of age, who appeared to be grasping an adult male penis which had ejaculated.

20. Your affiant responded to the above described post, telling donjuan045 that your affiant had an 8 year old daughter and maybe the two of us could work something out. Communication between donjuan045 and your affiant took place within the Motherless.com email messaging system for approximately two days. During this time, donjuan045 asked where we could meet and when; and suggested "a hotel up ur way". Donjuan045 also asked "will I get

a chance to touch her or just look at her....i would be so gentle and kind to her and would come bearing gifts". Donjuan045 indicated that he would provide your affiant with donjuan45's cell phone number so that they could speak and get to know each other.

21. On March 22, 2011, your affiant noted that donjuan045's profile on Motherless.com, showed that he had joined a group called "Very Cute Only". On the "Very Cute Only" group home page the moderator of the group had posted the following question: "Tell us what is the youngest you will fuck??". Your affiant observed that donjuan045 had posted an answer to this question four days prior, "i wont go below 5 not a definite but a fairbase line".

22. Donjuan045 provided your affiant with donjuan045.gmail com as his e-mailing address. Donjuan045 asked what type of clothing and items your affiant's daughter liked. Your affiant replied that my daughter like clothes from the Justice store. Donjuan45 replied that he would be purchasing some items for her at Justice.

23. On March 24, 2011, donjuan045 e-mailed your affiant cell phone number (609) 845-5723. Your affiant called the cell phone that day. A male answered who asked your affiant to refer to him as "Don". We both asked each other if the other was law enforcement. Don stated that he has a sexual attraction to little white girls. Don said that he had previously had sexual contact with an eight year old female. Don stated in this conversation and in subsequent conversations that any sexual contact he had with children was always initiated by the child. Don and your affiant have continued to speak on a daily basis since March 24, 2011. Don admitted in subsequent conversations that he has touched at least six to eight young girls. Don told your affiant that Don received oral sex from a four year old, that Don digitally penetrated an eight year old, and that he performed oral sex on two sisters; one six year old and the other eight years old.

During one telephone conversation between your affiant and Don, Don stated that he would be willing to perform oral sex on your affiant's daughter. Don also described two mixed race sisters, one four years of age and the other six years of age, who Don lets into a building on Saturdays for choir practice. Don stated that he has began to hug the girls, put his head on their shoulders, and give them high-fives, in an attempt to have them feel comfortable with him. Don stated that he is friends with the girls' grandmother and has asked the grandmother to bring the girls with her to have breakfast with him at his friend's restaurant. Don has indicated that he would have sexual physical contact with these sisters if he had the opportunity. Don explained to your affiant that it is a long process to gain the trust of children and that Don is patient.

24. A response to the administrative subpoena sent to the donjuan045@gmail account revealed that the email address of donjonesiii2003@yahoo.com is associated with that email account. A response to an administrative subpoena shows that the address for the Yahoo account donjonesiii2003 comes back to the subject premises address of 211 Arneys Mt. Road, Pemberton, New Jersey. An internet search of Donald Jones revealed an online resume in the name of Donald J. Jones III posted on the photobucket.com website, which listed a home address of 211 Arneys Mount Road, Pemberton, New Jersey. Jones' resume indicated that he had experience working at Little Caesar's Pizza and Domino's. In conversations between your affiant and Don, Don stated that he had worked at both pizza establishments. The State of New Jersey Sex Offender Registry revealed that Donald J. Jones, registered with an address of 211 Arney's Mount Road, Pemberton, New Jersey, is a level 2 child sex offender. Jones was convicted in 1993 of Aggravated Sexual Assault and Endangering the Welfare of a Child against a female under the age of 13. Review of Jones' criminal history also shows convictions in 2004

and 2009 for Endangering the Welfare of Children.

25. From March 29, 2011, up to and including April 5, 2011, donjuan045@gmail.com has e-mailed several videos and images containing child pornography to include children as young as infants, to your affiant's undercover email account. On April 3, 2011, Don sent your affiant one video containing child pornography from telephone number (609) 288-0961, a telephone number that donjuan045@gmail.com provided your affiant by text message to use to contact Don. These videos included as described below, the following:

(a) Video entitled "PTHC_NEW_Baby_Nice_Orgasm_From_4yo_Girl_2011.mpg"

This video features a pre-pubescent female child, approximately two to four years old wearing short pants and a short sleeve top. She has a pacifier in her mouth and is sitting on the lap of an adult male who is shirtless, has a grey beard and numerous tattoos on his arms. The male pulls the pre-pubescent female's shorts to the side, exposing her genitalia directly to the camera. Her legs are spread open and he begins to masturbate her with his right hand. She also masturbates herself during the course of the video.

(b) Video entitled "2010 pthc babyshivid frifam black mask 04(2).wmv"

This video features a pre-pubescent female child approximately one to two years old who is wearing a only a black hood and what appears to be a pull-up type of garment, which has been put to one side, fully exposing her vagina and anus to the camera. She is lying on her back. An adult male, with an erect penis, appears to be attempting to place his penis into her vagina. The pre-pubescent female is crying. The adult male pulls her pants up and around her knees, which are pressed against her chest, as he continues to attempt to penetrate her vagina with his penis. The adult male then turns the pre-pubescent

female over onto her stomach and presses his penis between her legs.

(c) Video entitled "008 Baby Lexxa Sexycum.mp4"

This video features a naked baby girl, less than one year old, lying on her back. An adult male is standing between her legs, which are spread open, exposing her genital area. The adult male masturbates and ejaculates on the baby's face, chest, abdomen and genital area.

(d) Video entitled "Buena.3gp"

This video features a naked pre-pubescent female lying on her back on a bed. A fully-clothed adult male is bending over her, kissing her on the mouth. The adult male then kisses her chest, abdomen, thighs and performs oral sex on her. The scene changes and the naked pre-pubescent female is on her stomach lying on the same bed. The adult male is now naked and climbs on top of the pre-pubescent female. He appears to be copulating with her from behind.

The above mentioned videos were made available for viewing to the reviewing magistrate judge. The videos will remain in the custody of law enforcement.

26. On March 29, 2011, donjuan045@gmail.com emailed your affiant and asked what town was next to his, so that Don could rent a motel/hotel to meet with your affiant's 8 year old daughter. Your affiant told Don that Warwick was the town next to his. On March 30, 2011, donjuan045@gmail.com e-mailed your affiant a confirmation of a reservation with the guest name Donald Jones, at the La Quinta Inn Suites, Warwick, Rhode Island. The check-in date of this reservation is listed as April 8, 2011 and the check-out date is listed as April 10, 2011. On April 6, 2011, Don told your affiant over the telephone that Don would be taking a greyhound

bus from Philadelphia to New York City, and then change buses in New York, and arrive in Providence at 2:25 p.m. on Greyhound bus number 3448 on Friday, April 8th.

27. On March 31, 2011, donjuan045@gmail.com communicated to your affiant's email that Don had mailed a package containing girl's clothing through the U.S. Mails, and that the package would be arriving at Inspector Stern's P.O. Box in Providence, Rhode Island by 1:00 p.m., April 1, 2011. Your affiant had previously provided his undercover P.O. box address to Don in response to Don offering to send clothing to the 8 year old daughter. Don also communicated to your affiant that Don wanted to see a photograph of your affiant's daughter wearing the clothing.

28. On April 1, 2011, your affiant intercepted a U.S.P.S. Express Mail Package from "D. Jones, 211 Arney's Mount Rd., Pemberton, NJ 08068", addressed to your affiant's undercover name and undercover P.O. Box in Providence, Rhode Island. The contents of the Express Mail Package were one pair of girl's underwear, one girl's skort, and one child's t-shirt, all purchased from Justice. Don had communicated to your affiant that Don had both visited a Justice retail store as well as the Justice online website and made purchases for your affiant's daughter from each. A response by Justice Security Department to an administrative subpoena confirmed that Don Jones made three separate online purchases from Justice's website and also revealed that the girl's clothing purchased by Don Jones was shipped by Justice to the subject premises, 211 Arney's Mount Road, Pemberton, New Jersey 08068.

29. U.S. Postal records show that on April 1, 2011, Don Jones called the Providence, Rhode Island P&DC retail unit and inquired as to the location of his Express Mail package. Don later told your affiant that Don was told by postal employees that his package was somewhere

*collected by 5/1/11
enter*

within the postal facility, but had not been scanned in yet. Don told your affiant that Don believed that weather contributed to the delay of the package and discussed the fact that he should receive a refund for his postage. On April 1, 2011, Don spoke with an undercover female police officer who Don believed was your affiant's 8 year old daughter. During his conversation, Don apologized to her for the package not arriving as he had promised. U.S. Postal records show that on April 2, 2011, Don Jones called the Providence, Rhode Island P&DC retail unit again to inquire as to the express package being delivered to the undercover P.O. Box. The Post Office captured telephone number (609) 288-0961, the same number given to your affiant by Don Jones and the same cell phone used to send a video containing child pornography (see paragraph 25, infra.). On April 5, 2011, Donald Jones requested and received a refund for his express package at the Mt. Holly, New Jersey post office. Don chatted with the postal employee and stated that he was going to Rhode Island on Friday, April 8th and stated that he was taking the greyhound bus.

30. On April 1, 2011, donjuan045@gmail.com sent the following message to your affiant's undercover email address: "this is the clip to show her!!!!!!!!!!!!!!!!!!!!!!". Attached to this message was the file entitled "Buena.3gp", more fully described in paragraph 25(d) of this affidavit. The video was approximately 1:10 in length. On multiple occasions, Don informed your affiant that Don kept his child pornography collection on several DVDs and flash drives. Don stated that two of his flash drives were 8 gigabytes in size. Don also told your affiant that Don had a laptop computer and that he uses his sister's Comcast connection when he is at her house to access the Internet. Don stated that he also uses his broadband card for internet access. A broadband card provides self contained access to the internet; it allows portable access to the internet. Don stated that it was a Verizon card.

31. Your affiant has communicated to Don Jones that your affiant will have custody of his daughter on Friday, April 8, 2011, until Sunday, April 10, 2011. Don has communicated to your affiant that Don will arrive in Rhode Island on Friday, April 8, 2011, and believes that he will meet both your affiant and his 8 year old daughter at his room at La Quinta and that the three will stay at the hotel for the weekend. Don also told your affiant that he can bring his laptop computer in order to play music that he believes the 8 year old girl will enjoy. Your affiant submits that there is probable cause to believe that Don Jones will bring both luggage for the 3 day visit and his laptop computer with him on April 8, 2011, to Rhode Island.

32. Surveillance and research have made your affiant aware that the premises located at 211 Arneys Mount Road, Pemberton, New Jersey 08068 are located in a rural area, with little vehicular traffic passing by. However, in his conversations with the target, Don Jones, Inspector Stern frequently heard noise associated with a busy street, including vehicular traffic. Don also told Inspector Stern that Don was staying with an elderly aunt and a nephew. On multiple occasions, Inspector Stern noted that Don was stepping outside to talk with Inspector Stern. On those occasions, Inspector Stern heard noise, including vehicular traffic, consistent with a busy street. On multiple occasions while speaking to Don, Inspector Stern heard a young male's voice in the background and Don would refer to him as his nephew and complain that the nephew played his music too loudly and that his nephew did not have a job. On multiple occasions while speaking to Don, Inspector Stern heard a voice in the background that sounded like an elderly female's voice.

33. Beginning on Monday April 4, 2011, U.S. Postal Inspectors performed surveillance on two subject premises associated with Donald Jones in New Jersey. With regard

to the premises located at 211 Arneys Mount Road, Pemberton, New Jersey 08068, surveillance reveals that this address is a house in the country, with a driveway. There is no city street or road close by the house. The target, Donald Jones is registered with the New Jersey Sex Offender registry at this address. Three of the Justice Store children's items were mailed to this address. In the online order, the "sold to" and "shipped to" addresses were the same; 211 Arneys Mount Road, Pemberton, New Jersey. This is also the address listed as the return address on the package containing the clothing shipped to your affiant in the express mail package.

Additionally, on March 31, 2011, Don informed your affiant that on April 1, 2011, your affiant would have Don's home address, referring to the expected arrival of the express mail package. With regard to surveillance on the subject premises located at 245 Washington Street, Mount Holly, New Jersey 08060, is listed with the U.S.P.S. as where Donald Jones receives mail. A database search on Lexus Nexus also lists Donald Jones' address as 245 Washington Street, Mount Holly, New Jersey 08060. This address is a duplex located on a busy street, which is consistent with the noise your affiant has frequently heard in the background during his conversations with Don. Across the street from this address is a church, which is consistent with Don's description of letting in two young girls into a building for choir practice. On April 4, 2011, Postal Inspector Anthony Fenu drove past the subject premises and saw a subject he believed to be Donald Jones, based upon his review of Donald Jones' New Jersey driver's license photograph. The male was standing at the front fence of the subject premises. On April 5, 2011, Donald Jones was observed walking away from 245 Washington Street, Mount Holly, New Jersey toward the Mt. Holly Post Office.


34. Based on the above information, your affiant submits that there is probable cause

to believe that Donald Jones committed the above listed offenses, and that he travels with his laptop computer. Your affiant further submits that there is probable cause to believe that there is evidence of the above listed crimes located on the laptop computer, the two listed cellular telephones, and any and all personal possession associated and with Donald Jones on April 8, 2011, in the District of Rhode Island.


CONCLUSION

35. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that Donald J. Jones has committed the below listed offenses, and that evidence of the commission of criminal offenses, namely, violations of 18 U.S.C. §§2423(b) and (f); 18 U.S.C. § 2422(b); 18 U.S.C. §§§ 2252(a)(2) and (b)(1) and 18 U.S.C. § 2225A, will be located in the described cellular telephones, the described laptop computer, and the belongings of Donald Jones as described above, and this evidence, listed in Attachment B to this affidavit, which is incorporated by reference, is contraband, the fruits of crime, or things otherwise criminally possessed, or property which is or has been used as the means of committing the foregoing offenses.

36. I therefore respectfully request that the attached arrest warrant be issued and the attached search warrants be issued authorizing the search and seizure of the items listed in Attachment B.


Jay E. Stern
United States Postal Inspector
United States Postal Inspection Service

Subscribed and sworn before me this 7th day of April, 2011


DAVID L. MARTIN
UNITED STATES MAGISTRATE JUDGE